Event summary of Session 7

Overview of Forensic Accountants' Proactive Roles in Fraud Risk Mitigation

Presented by Kelvin Cheong and Jessica Li, both of PwC

A. Introduction

- Common fraud risk areas

Internal fraud	
Any deliberate or dishonest acts committed by an employee for personal monetary gain.	
Financial Statement Fraud	• Accounting anomalies, such as growing revenues without a corresponding growth in cash flows; and • A surge in an organisation's performance in the final reporting period of a year.
Asset Misappropriation	• Cashier's ability to issue refunds without supervision; and • The existence of some branches / subsidiaries with high adjustments.
Data and Technology Abuse	• Access to databases by inappropriate persons; and • Removal of certain records before the end of the appropriate retention period.

External Fraud	
The risk of financial or reputational loss as a result of fraudulent acts committed by external parties.	
Disbursement Fraud	• Mismatched / fabricated receipts used for refund purposes; and • Same documents used for multiple relief / refund claim
Fraudulent Account Funding	• Cheques deposited, with amount withdrawn before cheque clearance (kiting); and • Cheques with altered amounts or beneficiary names.
Impersonation and Account Takeover	• This is on the rise. • Request for fund transfers through unlikely sources (e.g. social media); and • Phishing messages requesting personal information such as passwords.

B. Fraud Risk Management Framework

- Fraud Governance – It's More Than Just Compliance, i.e. more than just ticking the boxes

  - ➢ The need to develop a robust fraud risk management governance framework goes beyond regulatory compliance.

  - ➢ It is also necessary in order for an organisation to properly identify and defend against emerging threats that are growing in complexity.

  - ➢ Examples of key benefits of implementing a robust governance framework include:
    - delegation of clear accountabilities in organization;
    - enhanced cross-functions collaboration; and

- fraud loss reduction.

- **Fraud Risk Management Governance Framework, including the following five pillars, depending on companies' business**

Fraud Risk Management Framework	• Governance & oversight • Well-defined roles and responsibilities • Feedback loop between Lines of Defence • Firm-wide policies and procedures
Fraud Risk Assessment	• Periodic risk assessment (frequency should be risk-based) • Identify inherent risk • Inform effectiveness of controls in place • Consider both actual and potential incidents
Ongoing Monitoring	• Monitor compliance behaviours and detect potential compliance violations on an on-going basis • Develop data dashboards which consolidate and distil complex data into key risk indicators
Compliance / Risk Awareness Training & Communications	• Conduct customised face-to-face trainings on organisation's Code of Conduct and anti-fraud awareness matters • Regular communications / messages from senior management to emphasise "tone from the top"
Whistle-blower Programme	• Tipping seems to be an effective way to reveal potential fraud cases • Culture of zero tolerance • Respond to allegations of internal fraud matters

The first three elements are further explained below, given their importance.

- **Fraud Risk Management Framework Review**

  - Conducting a fraud risk management framework review will allow an organisation to identify and rectify potential issues in the design and operations of its fraud risk management program.

Governance Framework Review	• Review policies and procedures • Roles and function mapping; it is particularly important as different departments work in silo. • Review meeting minutes and management information reports
Interviews and Walkthroughs	• Identification of risks associated with key business processes • Controls identification & walkthroughs
Controls Review	• Controls design • Operations of controls
Sample Review and Analysis	• Review sampled transactions and underlying documents • Review Investigation Reports and findings
Relationship Analysis	• Review background check documents • Identify relationships
System Functionality	• Rule coverage gap analysis

Testing / Validation	• Validation of rule parameters and thresholds

- **Fraud Risk Assessment**

  - An enterprise fraud risk assessment enables an organisation to identify its risk exposures based on its business nature, size and relevant risk factors. As a result, it helps the organisation in formulating, enhancing and implementing fraud-related controls on a risk-based approach.

  - Key Objective

    - Fraud Risk Assessment is the basis of fraud risk management as it informs an organisation the type and level of risks it is exposed to. Regular performance of such assessment is particularly important for organisations which operate in different business segment/ territory, as risk assessment enables an organisation to deepen its understanding of its risk exposure in different business segment/ territory.

    - Key information to be obtained in a Fraud Risk Assessment includes:

      ✓ Identify inherent risks and latest market fraud risk exposures
      ✓ Assess the likelihood and significance of the inherent risks identified
      ✓ Determine whether controls are sufficient
      ✓ Determine what the residual risks are

    - Assessment results should be used to:

      ✓ Determine level of compliance testing required and facilitate planning of stress-testing on high risk areas;
      ✓ Determine whether additional controls need to be implemented;
      ✓ Determine level and types of ongoing monitoring required to monitor residual risks, and to track and to oversee the implementation of controls; and
      ✓ Feedback findings and recommendations to relevant business units.

  - Key Elements of a Fraud Risk Assessment

Methodology and Tools	Risk Assessment approach (e.g. survey) shall take into account the organisations' risk landscape, appetite and is commensurate with its operations and scale.
Data source and quality	Relevant information shall be ✓ extracted from multiple source of data (both internal / external); and ✓ utilised to provide the organisation a holistic view of fraud exposure Steps should also be taken to ensure quality of data used for the assessment.
Assessment result	Assessment results shall be: ✓ well-supported with justification, reviewed and approved

	✓ used for implementing mitigation measures, where necessary ✓ used to inform future risk appetite of the organisation
Documentation	Proper documentation of: ✓ Methodology ✓ Procedures ✓ Assumptions ✓ Justification of assessment results

- Fraud Risk Assessment Methodology

Fraud Risk Assessment can be mainly divided into three steps as below.

Planning and preparation	1) Past incident analysis • Review prior investigation cases (including those identified by peer organizations) and identify any common fraud schemes and trends. 2) Fraud risk questionnaire • Obtain understanding on the overall fraud risks for discussions in the deep dive sessions 3) Identify responsible process owners • Include relevant employees across different departments and grades. 4) Kick off meeting • The purpose is to let the fraud risk management function to understand the business processes before the deep dive sessions, and to get buy-in from different relevant parties.
Deep dive sessions	1) Identify the key inherent fraud risk by analyzing past fraud incidents and fraud risk questionnaires, interviewing a few key representatives, and assess both the impact and significance of the risk. 2) Map existing controls to key inherent fraud risks and evaluate the effectiveness of the control from both design perspective and operational perspective (stress testing). 3) Identify residual fraud risks, consider whether residual risk is within the risk appetite and whether additional controls are required.
Final presentation of results	1) Document the risk assessment results, for example, by heat map. Heat map is a useful tool to visualise the level of residual risks faced by an organisation, where an organisation's vulnerability to different fraud schemes is determined by plotting their likelihood and significance on the heat map

- Stress Testing – Key Objective

  - The key objective of performing stress testing is to assess the **operational effectiveness** of the internal control framework.

  - Stress-testing the current fraud prevention and detection internal controls enables a better understanding of their adequacy and effectiveness in day-to-day operations. Using a series of threat scenarios, an organisation can identify how fraud events impact its businesses and whether or not the control framework has been **transposed into operations** of the respective lines of businesses and support functions **as designed**.

    - ✓ Develop major fraud threat scenarios, and identify controls that can alleviate these situations
    - ✓ Review controls and identify vulnerabilities
      - ❖ Assess controls through walkthroughs and interviews
      - ❖ Conduct vulnerability and impact analysis
      - ❖ Conduct follow up sessions to confirm control gaps
    - ✓ Provide recommendations based on weaknesses identified

  - Provide recommendations based on weaknesses identified; here is an example

Governance	Propose alternative segregation duties
Culture & performance	Revamp approval processes and thresholds to hold senior management accountable and instil tone on the top
Risk management process	Suggest updates or creation of fraud policies, procedures or guidance if processes (including escalation and monitoring) in place are not aligned to policies
Infrastructure	Propose additional types of management information to be prepared at different levels / BUs

  - Key Learnings and Challenges

    - ✓ The intention of conducting risk assessments shall be clearly communicated by the organisation's senior management, as effective risk assessments require buy-in from business units

    - ✓ The organisation's senior management shall reiterate to all staff that risk assessment is a tool for the identification and management of fraud risks faced by the organisation, as opposed to an exercise to check the performance of business in managing these risks

    - ✓ The level of risk awareness and understanding may differ amongst business units / branches / subsidiaries. Aligning such understanding is important through communications and training for a meaningful and consistent assessment across the entire organisation.

- ✓ There shall also be a detailed and clear communication plan outlining how the risk assessment processes and new / enhanced control measures will be implemented across the organization

- ✓ Ownership of action items shall be clearly allocated and defined with effective tracking in place

- ✓ Periodic reviews shall be conducted to assess the effective of control measures in managing the potential fraud risks faced by the organisation.

➢ Common Observations

- Fraud risk assessment did not provide a holistic view of the organization's risk exposures, e.g. it only covered business areas where fraud incidents had occurred but did not assess the fraud risk exposure of other business areas;

- Insufficient rationale/ justification provided to support the fraud risk assessment results; and

- Fraud controls and/or response plan were not being developed in response to the issues identified and recommendations provided resulting from the fraud risk assessment.

- **Ongoing Monitoring – Monitoring & Detection Tools & Scenarios**

➢ With the implementation of tools within an organization to monitor and detect potential fraud behaviours and transactional activities, the organisation shall take appropriate steps to ensure the performance of the system is efficient and effective through testing, tuning and engaging personnel with appropriate knowledge.

➢ Key Elements of a Monitoring and Detection Tool:

- Data Completeness
- Data Accuracy
- Data Mapping
- Access control
- Thresholds and parameters
- Suppression rules
- Alert Profiling
- Scenario logic

➢ Common Observations

- No robust governance framework on ongoing monitoring and system tuning/ testing;
- Ongoing monitoring only covered static data and limited fraud scenarios (e.g. external fraud scenarios) and did not cover behavioural-related factors and different types of fraud that the organisation might be exposed to; and
- Periodic review was not conducted on the effectiveness of the ongoing monitoring measures, including relevance of scenarios.

C. Fraud Due Diligence

- In an investment lifecycle, apart from financial due diligence, it is equally important to pay attention to a broader set of risks, including potential acts of fraud by the investment target.

- Timing: When to look at fraud risks?

  - Typically, organisations start conducting relevant due diligence work prior entering a business deal. However, due diligence work can also be carried out throughout and after the business deal, see below:

    - Pre-deal due diligence
    - Post-deal compliance review
    - Remediation of internal controls gaps
    - Regulatory support
    - Compliance framework set-up

- Analysis: What can be done?

  - A wide range of techniques can be applied to assess the Fraud Compliance Framework of a target, depending on the nature of the business, deal stage, and level of access granted by the target.

    - Data room review
    - Interviews with key stakeholders, data analysts
    - Site visit compliance review
    - Forensic technology
    - Compliance intelligence
    - Economic analysis

  - Data Room Review: Review policies, procedures and relevant documents (e.g. fraud risk assessment results, fraud investigation reports etc.).

  - Interviews: Interview relevant stakeholders to understand the company's operations, its existing fraud compliance program (if any), its compliance culture and environment, interactions with employees, as well as external parties such as supplies and customers.

  - Site visit compliance review: On-site visit to walkthrough the key business processes in place, e.g. sales, purchases, payment request and approval, vendor tendering, contract signing and approval

  - Economic analysis: Conduct transactional sample testing on the risk sensitive accounts (e.g. entertainment expense account) that may contain potential transactions including but not limited to cash and petty cash payments, miscellaneous/other expense; travel and entertainment expenses, professional expenses, etc.

  - Forensic technology: Apply computer forensic technology, including email and electronic review tool, to identify suspicious relationships among customers, employees, and vendors, and question and analyse data sets and user files, if necessary

- Forensic Intelligence: Conduct forensic intelligence to gather information on the company's history, e.g. organisation, personnel structure, and key employees, etc. (refer to the next slide for further information on forensic intelligence)

- Response: What to do when a potential fraud issues arises?

  - If a potential compliance violation is identified during the course of the review, there are a number of options depending upon the severity of the problem including: (i) adjustment of the purchase price or modification to the purchase agreement; (ii) postponement of the transaction until the possible violation is resolved; and (iii) termination of the transaction.

- Overview of Forensic Intelligence

  - Forensic Intelligence is a process of gathering information on companies or individuals for a specific purpose through target research from various data sources - from traditional and social media and public records to sanctions/watch lists and litigation records and industry relationships. The information gathered concerns integrity or other "ref flag issues" relating to the target companies or individuals, which may empower organisations to make considerate and informed business decision.

    - Fraud
    - Bribery and Corruption
    - Money laundering and terrorist financing
    - Unethical business practices
    - Past and ongoing litigation
    - Tax Evasion

- How Forensic Intelligence Can Help

  Below are the common scenarios where forensic intelligence is required, and the key risk indicators that may be identified during the process.

  - Investing in new business, mergers and acquisitions
    - Opaque ownership information and/or ultimate beneficial owner;
    - Irregularities in the organisation's historical records;
    - Signs of financial distress or bankruptcy petitions; and
    - Ongoing litigation or breach of regulations

  - Establishing joint venture partnership / strategic alliance
    - Relationship with government and politically exposed persons;
    - Signs or references to favorable treatments received by government; and
    - References to bribery or corruption issues, etc.

  - Appointing senior management personnel
    - Inconsistency with the self-claimed track records;
    - Possible conflicts of interests;
    - Indication on the legitimacy of the source of funds; and
    - Indication on unethical behaviors, etc.

  - Recruiting / onboarding vendors, suppliers or distributors

- Potential conflicts of interests in ownership;
- Irregularities in the organisation's licensing information;
- References to bribery or corruption issues; and
- Ongoing litigation or breach of regulations, etc.

- Examples of Forensic Intelligence

Scope	Purposes
Corporate Registration Records Retrieval	• To confirm the target organisation's corporate registration and business license is in good standing; and • To identify ownership information and any irregularities in the organisation's historical records, e.g. frequent or recent change of shareholders or executives.
Employment History and Business Interests	• To identify any indications on the legitimacy of the source of funds, as well as any potential conflict of interest issues.
Political Exposure & Sanctions & Watch-lists Screening	• To identify any key individuals (including the senior executives) and/or ultimate beneficial owner(s) at the target organisation is or was a government official or equivalent, or they have been subject to any sanctions imposed by governments or regulators.
Litigation Records & Bankruptcy Records Review	• To identify any potential legal risks and/ or financial damages through association with the targets and any potential business interests or integrity issues for the target Individuals.
Adverse Media & Internet Records Review	• To identify any irregular activities or reputational issues associated with the targets (e.g. fraud, bribery, corruption, money laundering / terrorist financing activates).
Regulatory Records Review & Licensing Searches	• To check if the target organisation has the relevant business permits to carry out the claimed services, particularly the heavily regulated activities in the finance and legal industries; and • To identify any administrative penalties and/or fines from regulatory bodies in the relevant jurisdictions.
Site Visits	• To verify the existence and operational conditions (such as size, etc.) of the target organisation's registered location(s) and/or self-claimed operational site(s).

D. Fraud Analytics

- Fraud Analytics involves the use of tools / techniques to analyse large volume of data in order to detect suspicious or anomalous transactions.

- Preventative analytics blocks transactions in real-time, while detective analytics identifies the transactions post-event. When deciding which implementation should occur, an organisation should consider:

- Fraud risk appetite
- Ability to investigate, enforce, recover later
- Customer experience

(e.g. if you want to have zero fraud transactions, customers may not be happy about this.)

- Data analytics can also help management to comb through massive amounts of data, to come up with useful management information and statistics, which can provide clarity around priorities and resources required, and help with regulatory reporting.

- Types of Fraud Analytics

  - Specific Fraud Models: Out-of-the-box fraud analytics models designed for a specific purpose – e.g. credit card point of sale fraud
  - Behavioural Analytics: Identify red flag 'behaviour' (rather than fraud activity) to flag suspicious behaviour for follow-up
  - Scenario Driven Fraud Rules: Specific fraud rules to flag or block transactions based on previous incidents or perceived risk – e.g. payment requests to high risk countries such as Nigeria
  - Control Circumvention Analytics: Analytics designed to detect the circumvention of fraud controls – e.g. constantly submitting approval below limits
  - Supervised Machine Learning: Using previous known fraud cases to predict similar unknown cases, and/or as part of alert management.
  - Unsupervised anomaly detection: Advanced analytical techniques to detect items which are 'abnormal' compared to their peer segment
  - Supervised Machine Learning: Using previous known fraud cases to predict similar unknown cases, and/or as part of alert management.

- Examples of Analytics Technologies in the Market

  - Rules / Exception Based Systems
    - Have a set of in-built heuristics or anomaly rules that are based on typical 'fraud' scenarios. Can also incorporate risk scoring.
    - Generate 'alerts' / 'exceptions' when the rules are violated.
    - Alerts and exceptions are followed up by reviewers on a case basis.

  - Machine Learning & AI Based Models
    - Apply advanced analytics and other learning algorithms (e.g. text analysis).
    - Typically either 'supervised' (require training) or 'unsupervised' algorithms (do not require training).
    - Relatively new area for most corporate applications.

  - Network Analysis
    - Map 'relationships' between parties using a network style of representation.
    - Allow analysts to explore connections between parties (e.g. customers, agents and employees) that may not have been previously known.
    - Require relationship data to be gathered or maintained.

  - Real-world Challenges
    - Rules based systems can generate a large number of false positive alerts.

- Machine learning models require high quality data, training and expert skills to be productive.
- Only a small number of fraud typologies (e.g. credit card fraud) have a high detection probability (customer reports).
- Not all data is structured